INRIA

L'isomorphisme de Curry-Howard

Joëlle Despeyroux
INRIA Sophia-Antipolis

Module "Mécanisation des Preuves"
Dea d'informatique, Nice, janvier-mars 2000

Curry-Howard dans le λ-calcul simple

Logique propositionelle:

$$\Rightarrow_i: \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \Rightarrow_e: \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\wedge_i : \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \wedge_{e1} : \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \wedge_{e2} : \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\vee_{i1} \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \vee_{i2} \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \qquad \vee_e \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

λ-calcul simplement typé:

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x : A.\ t : A \to B} \qquad \frac{\Gamma \vdash t : A \to B \quad \Gamma \vdash a : A}{\Gamma \vdash (t\ a) : B}$$

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B}{\Gamma \vdash (a, b) : (A \times B)} \qquad \frac{\Gamma \vdash t : (A \times B)}{\Gamma \vdash \mathrm{fst}\ t : A} \qquad \frac{\Gamma \vdash t : (A \times B)}{\Gamma \vdash \mathrm{snd}\ t : B}$$

$$\frac{\Gamma \vdash a : A}{\Gamma \vdash \mathrm{inl}\ a : (A + B)} \qquad \frac{\Gamma \vdash b : B}{\Gamma \vdash \mathrm{inr}\ b : (A + B)}$$

$$\frac{\Gamma \vdash t : A + B \qquad \Gamma, a : A \vdash t_1 : C \qquad \Gamma, b : B \vdash t_2 : C}{\Gamma \vdash \mathrm{case}\ t\ \mathrm{of\ inl}\ a \Rightarrow t_1 \mid \mathrm{inr}\ b \Rightarrow t_2 : C}$$

Règles de réduction:

correspondent aux éliminations des coupures dans la logique

$$(\lambda x : A.M \quad N) \hookrightarrow_\beta M[N/x]$$
$$\mathrm{fst}(M, N) \hookrightarrow M \qquad \mathrm{snd}(M, N) \hookrightarrow N$$
$$\mathrm{case\ inl}\ t\ \mathrm{of\ inl}\ a \Rightarrow t_1 \mid \mathrm{inr}\ b \Rightarrow t_2 \hookrightarrow t_1[t/a]$$
$$\mathrm{case\ inr}\ t\ \mathrm{of\ inl}\ a \Rightarrow t_1 \mid \mathrm{inr}\ b \Rightarrow t_2 \hookrightarrow t_2[t/b]$$
$$(\mathrm{fst}(M), \mathrm{snd}(M)) \hookrightarrow_\eta M$$

Les Systèmes de Types Purs (PTS)

$termes \;\; M \;\; ::= x \mid c \mid \lambda x : M.M' \mid (M \;\; M') \mid \Pi x : M.M'$
Un PTS est défini par la donnée d'un triplet $(\mathcal{S}, \mathcal{A}, \mathcal{R})$ où $\mathcal{S} \subset \mathcal{C}$, $\mathcal{A}$ est un ens d'axiomes $(c : s)$ où $c \in \mathcal{C}$ et $s \in \mathcal{S}$, et $\mathcal{R}$ est un ens de triplets (s_1, s_2, s_3) avec $s_i \in \mathcal{S}$.

$$ax \;\; \vdash c : s \quad (c : s) \in \mathcal{A}$$

$$var \;\; \frac{\Gamma \vdash A : s}{\Gamma, x : A \vdash x : A} \; x \notin \Gamma$$

$$aff \;\; \frac{\Gamma \vdash A : B \qquad \Gamma \vdash C : s}{\Gamma, x : C \vdash A : B} \; x \notin \Gamma$$

$$lam \;\; \frac{\Gamma, x : A \vdash M : B \qquad \Gamma \vdash (\Pi x : A.B) : s}{\Gamma \vdash \lambda x : A.M \;\; : \;\; \Pi x : A.B}$$

$$app \;\; \frac{\Gamma \vdash M : \Pi x : A.B \qquad \Gamma \vdash N : A}{\Gamma \vdash (M \;\; N) : B[N/x]}$$

$$prod \;\; \frac{\Gamma \vdash A \;\; : \;\; s_1 \qquad \Gamma \vdash B \;\; : \;\; s_2}{\Gamma \vdash \Pi x : A.B \;\; : \;\; s_3} \; (s_1, s_2, s_3) \in \mathcal{R}$$

$$conv \;\; \frac{\Gamma \vdash A \;\; : \;\; B \qquad \Gamma \vdash B' \;\; : \;\; s \qquad B =_\beta B'}{\Gamma \vdash A \;\; : \;\; B'}$$

Le λ-cube est un sous-ens des PTS, où $(s_1, s_2) = (s_1, s_2, s_2)$.

Déduction Naturelle dans LF

$$\Rightarrow_I: \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \Rightarrow_E: \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\begin{array}{ll} Prop & : * \\ \Rightarrow & : Prop \to Prop \to Prop \\ T & : Prop \to * \\ \Rightarrow_i & : \Pi A, B : Prop.(T(A) \to T(B)) \to T(A \Rightarrow B) \\ \Rightarrow_e & : \Pi A, B : Prop.T(A \Rightarrow B) \to T(A) \to T(B) \end{array}$$

Exemples:

$\vdash (\Rightarrow_i \ A \ A \ (\lambda x : T(A).x)) : T(A \Rightarrow A)$ représente $\dfrac{A \vdash A}{\vdash A \Rightarrow A}$

$\vdash (\Rightarrow_i \cdots (\Rightarrow_i \cdots (\lambda x : T(A).\lambda y : T(B).x)) : T(A \Rightarrow (B \Rightarrow A))$

représente $\dfrac{\dfrac{A, B \vdash A}{A \vdash B \Rightarrow A}}{\vdash A \Rightarrow (B \Rightarrow A)}$

Déduction Naturelle dans LF *(suite)*

$$\neg_I : \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A} \qquad \neg_E : \frac{\Gamma \vdash A \qquad \Gamma \vdash \neg A}{\Gamma \vdash \bot}\,(\bot_I) \qquad \bot_E : \frac{\Gamma \vdash \bot}{\Gamma \vdash A}$$

$$\wedge_I : \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \wedge_{E1} : \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \wedge_{E2} : \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\vee_{I1} : \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \vee_{I2} : \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

$$\vee_E : \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

$$\begin{array}{ll} tt, \bot & : Prop \\ \neg & : Prop \to Prop \\ \wedge, \vee & : Prop \to Prop \to Prop \end{array}$$

$$\begin{array}{ll}
\neg_i & : \Pi A : Prop.(\Pi B : Prop.T(A) \to T(B)) \to T(\neg A) \\
\neg_e & : \Pi A : Prop.T(A) \to T(\neg A) \to \Pi B : Prop.T(B) \\
tt_i & : T(tt) \\
\bot_e & : \Pi A : Prop.T(\bot) \to T(A) \\
\wedge_i & : \Pi A, B : Prop.T(A) \to T(B) \to T(A \wedge B) \\
\wedge_{e1} & : \Pi A, B : Prop.T(A \wedge B) \to T(A) \\
\wedge_{e2} & : \Pi A, B : Prop.T(A \wedge B) \to T(B) \\
\vee_{i1} & : \Pi A, B : Prop.T(A) \to T(A \vee B) \\
\vee_{i2} & : \Pi A, B : Prop.T(B) \to T(A \vee B) \\
\vee_e & : \Pi A, B, C : Prop.T(A \vee B) \to (T(A) \to T(C)) \to \\
 & \quad (T(B) \to T(C)) \to T(C)
\end{array}$$

Déduction Naturelle dans LF *(suite)*

$$\forall_i : \frac{\Gamma \vdash P}{\Gamma \vdash \forall x.P}\ x \notin \Gamma \qquad \forall_e : \frac{\Gamma \vdash \forall x.P}{\Gamma \vdash P[a/x]}$$

Mieux écrit: $\forall_i : \dfrac{\Gamma \vdash P(t)}{\Gamma \vdash \forall x.P(x)}\ x \notin \Gamma \qquad \forall_e : \dfrac{\Gamma \vdash \forall x.P(x)}{\Gamma \vdash P(a)}$

On représente $\forall x.P(x)$ par $\forall(\lambda x : i.P(x))$.
La substitution est modélisée par l'application méta.

$$\begin{aligned}
\forall &: (var \to Prop) \to Prop \\
\forall_i &: \Pi P : var \to Prop.(\Pi x : var.T(P\ x)) \to T(\forall P) \\
\forall_e &: \Pi P : var \to Prop.T(\forall P) \to \Pi x : var.T(P\ x)
\end{aligned}$$

Plus de 'side condition' sur les variables
var objet = var méta

syntaxe abstraite d'ordre supérieur (hoas)

$$\exists_I : \frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x.\ A(x)} \qquad \exists_E : \frac{\Gamma \vdash \exists x.\ A(x) \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ (x \notin \Gamma, B)$$

$$\begin{aligned}
\exists &: (var \to Prop) \to Prop \\
\exists_i &: \Pi A : var \to Prop.\Pi x : var.T(A\ x) \to T(\exists A) \\
\exists_e &: \Pi A : var \to Prop.\Pi B : Prop.T(\exists A) \to \\
&\quad (\Pi x : var.T(A\ x) \to T(B)) \to T(A)
\end{aligned}$$

Isomorphisme de Curry-Howard étendu

Logique propositionelle:

$$\Rightarrow_i: \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \Rightarrow_e: \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x : A.\ t : A \to B} \qquad \frac{\Gamma \vdash t : A \to B \quad \Gamma \vdash a : A}{\Gamma \vdash (t\ a) : B}$$

Calcul des prédicats ($\Rightarrow$ et $\forall$):

$$\forall_I : \frac{\Gamma \vdash B}{\Gamma \vdash \forall x.\ B}\ (x \notin \Gamma) \qquad \forall_E : \frac{\Gamma \vdash \forall x.\ B}{\Gamma \vdash B[t/x]}$$

$\Rightarrow$ et $\forall$ sont représentés par le même opérateur Π, où on étend le type de la variable x à tout type A:

$$\frac{\Gamma, x : A \vdash M : B \qquad \Gamma \vdash (\Pi x : A.B) : s}{\Gamma \vdash \lambda x : A.M\ :\ \Pi x : A.B} \qquad \frac{\Gamma \vdash M : \Pi x : A.B \qquad \Gamma \vdash N : A}{\Gamma \vdash (M\ N) : B[N/x]}$$

Règle de réduction:

$$(\lambda x : A.M\ \ N) \hookrightarrow_\beta M[N/x]$$

Curry-Howard étendu (suite)

Logique propositionelle:

$$\wedge_i : \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \wedge_{e1} : \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \wedge_{e2} : \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\vee_{i1} \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \vee_{i2} \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \qquad \vee_e \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B}{\Gamma \vdash (a, b) : (A \times B)} \qquad \frac{\Gamma \vdash t : (A \times B)}{\Gamma \vdash \text{fst } t : A} \qquad \frac{\Gamma \vdash t : (A \times B)}{\Gamma \vdash \text{snd } t : B}$$

$$\frac{\Gamma \vdash a : A}{\Gamma \vdash \text{inl } a : (A + B)} \qquad \frac{\Gamma \vdash b : B}{\Gamma \vdash \text{inr } b : (A + B)}$$

$$\frac{\Gamma \vdash t : A + B \qquad \Gamma, a : A \vdash t_1 : C \qquad \Gamma, b : B \vdash t_2 : C}{\Gamma \vdash \text{case } t \text{ of inl } a \Rightarrow t_1 \mid \text{inr } b \Rightarrow t_2 : C}$$

Calcul des prédicats ($\wedge$, $\vee$ et $\exists$):

$$\exists_I : \frac{\Gamma \vdash B[a/x]}{\Gamma \vdash \exists x.\ B} \qquad \exists_E : \frac{\Gamma \vdash \exists x.\ B \qquad \Gamma, B[a/x] \vdash C}{\Gamma \vdash C}\ (x \notin \Gamma, C)$$

$\wedge$ et $\exists$ sont représentés par le même opérateur Σ:

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B[a/x]}{\Gamma \vdash (a, b) : \Sigma x : A.B} \qquad \frac{\Gamma \vdash t : \Sigma x : A.B \qquad \Gamma, u : B[a/x] \vdash t'[a/x] : C}{\Gamma \vdash \text{case } t \text{ of } (x, u) \Rightarrow t' : C}$$

Note: fst et snd ne sont pas des cas particuliers du case.
Σ n'existe pas dans certaines théories typées.

Règle de réduction:

case (a, b) of $(x, u) \Rightarrow t' \hookrightarrow t'[a/x][b/u]$

Curry-Howard sur les données

formule de $L \rightarrow$ un type d'un λ-calcul (spécification),
preuve (dérivation) dans $L \rightarrow$ un terme de ce λ-calcul.

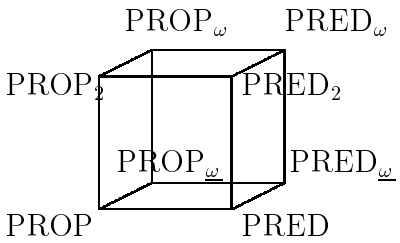
Exemples.

- $(even\ 0)$ est un type, ou spécification: "0 est pair."
- $even_S$ est un terme de type $\forall n : nat.(even\ n) \rightarrow (even\ (S\ (S\ n)))$, permettant de construire des preuves
- $\lambda n : nat.\lambda p : (even\ n) \rightarrow (even\ (S(S\ n)))$ est une fonction qui prend un entier n et une preuve p du fait que $(even\ n)$ et rend une preuve de $(even\ (S(S\ n)))$, donnée par le terme: $(even_S\ n\ p)$, et correspondant à la dérivation:

$$\frac{\begin{array}{c} p \\ (even\ n) \end{array}}{(even\ (S(S\ n)))}\ even_S$$

Isomorphisme de Curry-Howard - Le cube logique

PROP: logique propositionnelle / PRED: logique des prédicats.



Le cube logique est isomorphe au λ-cube:
T: formule de $L_i \rightarrow$ un type de λ_i.

Thm *(Iso. de Curry-Howard)* Le terme t de λ_i représente une preuve de la formule f de L_i ssi t est de type $T(f)$ dans λ_i.

Exemple. F, langage fonctionnel typé polymorphe $(\Box, *)$, correspond à PROP$_2$, logique propositionelle étendue par une quantification sur les var. de proposition $(\forall A, B : (A \wedge B) \Rightarrow A)$.